DEPARTMENT POLICY

POLICY # 113

SUBJECT: DSCYF Communications Networks

EFFECTIVE DATE: 10/1/97

I. Purpose

This document sets forth the policy of the Department of Services to Children, Youth and Their Families (DSCYF) for proper use of DSCYF communications networks: including computer systems, Internet access, and the electronic mail system. Nothing in this document shall be construed to contradict or override the *State of Delaware State Information Transport Network (SITN) Acceptable Use Policy (see attached).* This document addresses acceptable use of the Department's telecommunications network and stand-alone workstations.

II. Scope

This policy puts forth guidelines to be followed when using DSCYF information systems, and applies to all users of DSCYF information systems.

III. Definitions

Acceptable and Unacceptable Uses are defined in the *SITN Acceptable Use Policy Document*.

IV. Procedures

A. Notification

1. Warning Banner

The following warning banner will appear on all DSCYF Banyan networks.

This system is for the use of authorized employees and contractors only. Individuals using this computer system are subject to having their activity on this system monitored and recorded. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible conduct of criminal activity, the Department may provide the evidence of such activity to law enforcement officers. Individuals using this system

without authorization, or in excess of their authorization, are subject to disciplinary and/or legal action. Anyone using this system expressly consents to comply with DSCYF Guidelines for Electronic Mail and Computer Systems Use. A copy of the Guidelines is available on the DSCYF Intranet Site. (This policy will serve as the document referenced above.)

B. Guidelines for Electronic Mail Use

1. The electronic mail and other DSCYF information systems shall not be used in a way that may be disruptive, offensive to others, or harmful to morale.

2. There shall be no display, storage, or transmission of sexually explicit images, messages or cartoons, or any transmission or use of electronic mail communications that contain ethnic slurs, racial epithets, or anything that may be construed as harassment or disparagement of others (even if made in jest) based on their race, national origin, sex, sexual orientation, age, disability, or religious or political beliefs.

3. Employees may use the information systems for DSCYF business only (including professional development). The electronic mail and computer systems shall not be used to solicit or proselytize others for commercial ventures, religious or political causes, outside organizations, or other non-job-related solicitations.

4. All messages and files are DSCYF records. DSCYF reserves the right to access and disclose all messages and files stored on its systems or sent over its electronic mail system for any purpose.

5. For privacy reasons, it is not acceptable for employees to gain access to another employee's computer files without the latter's express permission. However, DSCYF management reserves the right to enter an employee's computer files whenever there is a business need to do so.

6. Employees using electronic mail and DSCYF information systems shall take appropriate steps to safeguard the confidentiality of client information. Nothing in this document shall be construed to contradict or override the *Departmental Confidentiality Policy.*

C. Monitoring (see Remedial Action in the *SITN Acceptable Use Policy Document)*

1. Authorization To Monitor

   Authorization to monitor or view any information created or used by a user of the computer system may only be given by the Secretary of DSCYF. The Secretary will specify: (a) the names of the users to be monitored, (b) the items to be monitored, (c) the items to be reported back to the Secretary, (d) the specific person who shall do the monitoring, and (e) the start and end dates for which the monitoring is authorized.

2. Monitoring

   Monitoring of information created or used by a user of the information system will only be conducted by a trained system administrator. This administrator shall do only the monitoring approved by the Secretary and shall treat all information obtained confidentially.

3. Information to be Monitored

   Information that can be monitored under this policy includes any e-mail messages in the user's message store, files stored by the user on the network, PC hard drive, and removable media, as well as monitoring how the PC is actually being used and the actual screens being displayed on the PC.

4. User Notification

   Users to be monitored will not receive specific notification of that possibility. The banner which will be displayed for all users at network sign-on time is considered to be that notification.

V. Implementation

This policy becomes effective October 1, 1997.